

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

LISA CHAPMAN,
New Kensington, PA
individually and on behalf of
a class of similarly situated individuals

Plaintiff,

v.

INSIGHT GLOBAL, INC
4170 Ashwood Dunwoody Road
Atlanta, GA 30319

Defendant.

Civil Case No.: 1:21-cv-824-CCC

**FIRST AMENDED CLASS
ACTION COMPLAINT**

JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Lisa Chapman (“Plaintiff”), individually and on behalf of the Classes defined below of similarly situated persons, bring this Class Action Complaint and allege the following against Defendant Insight Global, Inc. (“Insight”), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach

(the “Data Breach”) involving Insight, which collected and stored certain private health information (“PHI”) of the Plaintiff and the putative Class Members, all of whom have PHI on Insight and DOH servers.

2. The PHI compromised in the Data Breach included highly-sensitive information including but not limited to name, gender, phone number, sexual orientation, family size, and health data.

3. The Data Breach was a direct result of Defendant’s failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers’ PHI.

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant’s inadequate safeguarding of Class Members’ PHI that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party and precisely what specific type of information was accessed.

PARTIES

5. Plaintiff Lisa Chapman is an adult individual and citizen of the Commonwealth of Pennsylvania who resides in New Kensington, Westmoreland County, Pennsylvania.

6. Defendant Insight is an employment staffing company with its principal place of business and headquarters at 4170 Ashford Dunwoody Road, Atlanta, Georgia 30319. Insight conducts business throughout Pennsylvania.

7. At all times relevant hereto, Plaintiff was a citizen of the Commonwealth of Pennsylvania whose PHI was disclosed without authorization to unknown third parties as a result of the data disclosure described above.

JURISDICTION AND VENUE

8. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds \$5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

9. This court has personal jurisdiction over Defendant because it is authorized to and does conduct substantial business in this District.

10. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose throughout the Commonwealth of Pennsylvania, including in Dauphin County, which is in the Middle District of Pennsylvania.

COMMON FACTUAL ALLEGATIONS

11. Plaintiff and the proposed Class are individuals who were either diagnosed with or in close proximity to individuals diagnosed with COVID-19, and who were contacted by Insight for the purposes of contact tracing to understand, address, and potentially slow the spread of COVID-19.

12. “Contact tracing” is the process of notifying individuals of exposure to COVID-19, addressing questions and concerns, referring for testing, encouraging self-quarantine, monitoring of symptoms, and assessing the need for additional supportive services during the quarantine period.¹

13. Plaintiff brings this class action against Defendant for Defendant’s failure to properly secure and safeguard protected health information as defined by the Health Insurance Information Portability and Accountability Act (“HIPAA”), medical information, and other personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other members of the class that such information had been compromised.

Insight Global’s Contact Tracing Program

¹ <https://www.cdc.gov/coronavirus/2019-ncov/global-covid-19/operational-considerations-contact-tracing.html> (last accessed May 4, 2021).

14. Insight is an employment staffing company headquartered in Atlanta, Georgia, which does business throughout Pennsylvania.

15. Insight was contracted by Pennsylvania Department of Health (“DOH”) to perform contact tracing analysis and other services beginning in 2020.

16. There was no competitive bidding process for the contract, which totaled approximately \$23 million, between Insight and DOH.

17. DOH obtained COVID-19 test results for all persons who tested positive for the disease via the PA National Electronic Disease Surveillance System (“PA-NEDSS”), a system which “facilitates electronically transferring public health surveillance data from the healthcare system to public health departments.”²

18. At all times relevant hereto, DOH was a covered entity under the terms of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and asserted that it keeps the health information of Pennsylvanians private. *See* Exhibit A, “Commonwealth of Pennsylvania Department of Health (DOH) Notice of Privacy Practices for Protected Health Information.”

19. Insight is a business associate of DOH under the terms of HIPAA.

² <https://www.health.pa.gov/topics/Reporting-Registries/Pages/PA-NEDSS.aspx> (last accessed May 4, 2021).

20. As a business associate of DOH, Insight was required to “establish and maintain appropriate safeguards to prevent any use or disclosure of PHI.” *See* Exhibit B, “Commonwealth of Pennsylvania Business Associate Appendix – HIPAA Compliance.”

21. DOH at all times relevant hereto asserted that “all communication related to contact tracing is private and confidential” and that “your information will stay confidential.”³ It is believed and averred that DOH’s assertions to Plaintiff and Class members were based on promises and representations made to it by Insight Global.

22. Over a period of months in 2020 and 2021, employees of Insight contacted residents of the Commonwealth of Pennsylvania including Plaintiff and the proposed Class and obtained sensitive and protected health information including but not limited to name, gender, phone number, sexual orientation, gender presentation, family size, and health data (hereinafter, collectively, “PHI”).

Insight Global’s Unsecure Data Management and Disclosure of Data Event

23. Plaintiff and Class Members provided their PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply

³ <https://www.health.pa.gov/topics/disease/coronavirus/Pages/Contact-Tracing.aspx> (last accessed May 4, 2021).

with its obligations to keep such information confidential and secure from unauthorized access, and to participate in the contact tracing program that ostensibly existed to aid in mitigating the spread of COVID-19.

24. However, Insight failed to secure the PHI of the individuals it contacted.

25. Insight's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date they disclosed the incident.

26. Insight maintained unsecure spreadsheets, databases, and or/documents containing the PHI of tens of thousands of Class Members.

27. These documents were widely available to the public through a Google search and did not require a password, log in, or any kind of authentication in order to be viewed.

28. Based upon information and belief, Insight was aware that its employees were using their personal laptops and otherwise using unsecure data storage and communications methods as early as November 2020. *See* Exhibit C, emails exchanged between employees of Insight.

29. Insight failed to take any action to secure the PHI of Plaintiff or other class members until at least April 21, 2021. *See* "Notice of Data Event Related to

Pennsylvania Contact Tracing” at Exhibit D (printed from Insight’s website on May 5, 2021).

30. Insight failed to take any action to notify Plaintiff or other class members of this breach until at least April 29, 2021. *See* Exhibit D.

31. This was not the first opportunity Insight had to correct the issue, *see* Exhibit C. Additionally, at least one individual, a former employee of Insight, attempted to bring the non-compliant issues to correction within the company and was ignored. *See* Exhibit E, an email from a former employee of Defendant insight to the Pennsylvania DOH Office of Legal Counsel.

32. Despite this dissemination of notice and action to secure, Insight continues to place class members at risk, as certain individuals’ data remained unsecured “more than a month after Insight Global stated its data was secured.”⁴

33. Defendant has acknowledged the sensitive and confidential nature of the information here at issue. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PHI can pose significant financial and privacy risks, and that they may not disclose and must take reasonable steps to protect such PHI from improper release and disclosure.

⁴ <https://healthitsecurity.com/news/insight-global-calls-on-former-employees-to-secure-pii-data-breach> (Last Accessed August 26, 2021)

34. Despite these acknowledgements and averments that all PHI obtained in connection with COVID-19 contact tracing would be kept private and confidential, Defendant failed to take appropriate or even the most basic steps to protect the PHI of Plaintiffs and other class members from being disclosed.

Plaintiff and the Class Have Suffered Injury as a Result of Insight's

Data Mismanagement

35. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and other class members' PHI has been and is now in the hands of the general public including thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiffs and other class members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

36. Plaintiffs and other class members have had their most personal, sensitive and private information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

37. As an illustrative example, since disclosure of the Data Breach, Plaintiff Chapman has received mysterious and off-putting telephone calls and

messages on multiple days (sometimes multiple times a day) in which the caller refused to identify himself until Plaintiff provided personal information.

38. These calls have occurred daily at varying times, and have affected both a cell number and a work number that Plaintiff Chapman has. The phone number is consistent and appears to be an automated number or a “robocaller” used in phishing or telephone scammer schemes.

39. These calls did not begin until after disclosure of the Data Breach, and phone numbers were collected (and subsequently exposed) in Defendant’s initial charge and contacts with Plaintiffs. The subsequent fallout from this Data Breach is already apparent to Plaintiff Chapman, who must utilize considerable time and effort to scrutinize incoming phone calls and be “on watch” for other consequences of her divulged information.

40. Plaintiff and Class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety, as they will be at risk for falling victim for cybercrimes for years to come.

41. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3)

more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

42. Once PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Insight's conduct. Further, the value of Plaintiff's and Class members' PHI has been diminished by its exposure in the Data Breach.

43. As a result of Insight's failures, Plaintiff and Class members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

44. Plaintiff and Class members are also at a continued risk because their information remains in Insight's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as the Insight fails to undertake the necessary and appropriate security and training measures to protect individuals' PHI.

45. Plaintiff Chapman and the Class suffered actual injury from having PHI compromised as a result of Insight's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value

of their PHI, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

46. For the reasons mentioned above, Insight's conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class these significant injuries and harm.

47. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PHI and for failing to provide timely, accurate, and adequate notice to Plaintiffs and other class members that their PHI had been compromised.

48. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, publicity given to private life, and breach of implied contract.

CLASS ACTION ALLEGATIONS

49. Plaintiff bring this action on behalf of herself and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

50. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons in the United States whose PHI was compromised in the Data Breach as disclosed by Insight on April 29, 2021 (the “Nationwide Class”).

51. Plaintiffs propose the following Subclass definition, subject to amendment as appropriate:

All persons in the Commonwealth of Pennsylvania whose PHI was compromised in the Data Breach as disclosed by Insight on April 29, 2021 (the “Pennsylvania Subclass”).

52. Excluded from the Classes are Defendant’s officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

53. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

54. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Classes consist of at least thousands of people whose data was compromised in the Data

Breach.

55. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common question of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PHI;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PHI;
- f. Whether Defendant breached its duty to Class Members to safeguard their PHI;
- g. Whether computer hackers obtained Class Members' PHI in the Data Breach;

- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Defendant's conduct was negligent;
- j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- k. Whether Defendant's acts breaching an implied contract they formed with Plaintiff and the Class Members;
- l. Whether Defendant violated the Federal Trade Commission Act ("FTC Act");
- m. Whether Defendant violated the Health Insurance Portability and Accountability Act ("HIPAA");
- n. Whether Defendant violated Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, *et. seq.*;
- o. Whether Defendant was unjustly enriched to the detriment of Plaintiff and the Class;
- p. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

56. Typicality. Plaintiff's claims are typical of those of other Class

Members because Plaintiff's PHI, like that of every other Class Member, was compromised in the Data Breach.

57. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

58. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

59. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect

to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

60. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

61. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PHI;
- b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;
- c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PHI; and

- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

62. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT

Negligence

(On Behalf of Plaintiff individually and on Behalf of the Nationwide Class and/or Pennsylvania Subclass)

63. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

64. By accepting Plaintiff's and other class members' non-public personal information, Defendant Insight assumed a duty to use reasonable and, at the very least, industry standard care to secure such information against disclosure, theft, and misuse.

65. Defendant Insight breached its duty of care in failing to adequately, or in any meaningful way, secure and protect the PHI of Plaintiff and other class members from disclosure, theft, and misuse.

66. Defendant Insight further breached its duty of care by failing to promptly, clearly, and accurately inform Plaintiff and other class members that their personal information had been disclosed.

67. Plaintiff and other members of the class have suffered injuries that may include: (i) the lost or diminished value of PHI; (ii) out of pocket expenses and other costs in terms of time and effort that have gone into methods of prevention, monitoring, detection, contesting fraudulent claims, and repairing the impact of the Data Breach, including potential identity theft, tax fraud, and/or unauthorized use of their PHI, from the date of disclosure to the present; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their PHI, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI in their continued possession; and (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Members of the Classes, including ongoing credit monitoring.

68. As a direct and proximate result of the negligence of Defendant Insight in failing to take adequate steps to protect the personal information in its care, Plaintiff and other members of the class now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's failures.

69. As a direct and proximate result of the negligence of Defendant Insight in failing to take adequate steps to protect the personal information in their care, Plaintiff and other class members have had their most personal and private information disseminated to the public at large and now experience and will continue to experience emotional pain and mental anguish and embarrassment.

70. The publicly accessible posting of Plaintiff's and other class members' PHI combined with the complete and total lack of any security measures whatsoever including but not limited to a login requirement, password protection, or encryption evidences a reckless and wanton disregard for the private information of Plaintiff and other class members, which entitles them to punitive damages.

71. As a direct and proximate result of Insight's negligence, Plaintiff and the Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND COUNT

**Publicity Given to Private Life
(On Behalf of Plaintiffs individually and on Behalf of the Nationwide Class
and/or Pennsylvania Subclass)**

72. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

73. As alleged herein, from 2020 through 2021, Defendant caused the PHI of Plaintiff and other members of the class to be widely, openly, and generally available to the public despite their duty to keep this information private and confidential.

74. Specifically, Defendant disseminated or caused to be disseminated the Plaintiff's private and protected information including but not limited to their COVID-19 statuses.

75. Such information is private information, the disclosure of which would be highly offensive to a reasonable person and which is not of legitimate concern to the public.

76. Plaintiff believes and therefore avers that the disclosure of private information shows reckless and wanton disregard for their privacy, which entitles Plaintiff and the Class to punitive damages.

77. As a direct and proximate result of Insight's disclosure of Plaintiff's and Class Members' PHI, Plaintiffs and the Class Members have been injured as

described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD COUNT

Breach of Implied Warranty (On Behalf of Plaintiffs individual and on Behalf of the Nationwide Class and/or Pennsylvania Subclass)

78. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs.

79. Defendant provided Plaintiff and Class Members with an implied contract to protect and keep confidential Defendant's current, former, and prospective contact tracing participants' private, nonpublic personal health information when they gathered the information from each of their current, former, and prospective contact tracing participants.

80. Plaintiff and Class Members would not have provided their personal health information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's current, former, and prospective contact tracing participants' private personal health information.

81. Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal health information in exchange for participation in the contact tracing system, used in aid to mitigate the spread of COVID-19, provided by Defendant.

82. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal health information provided to them about Plaintiff and Class Members.

83. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, pray for judgment as follows:

- a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;
- b. For equitable relief enjoining Insight from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI;
- c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PHI compromised during the Data Breach;

- d. For an order requiring Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class(es);
- e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- f. For an award of punitive damages, as allowable by law;
- g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h. Pre and post-judgment interest on any amounts awarded; and
- i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 27, 2021

Respectfully Submitted By:

SHUB LAW FIRM LLC

/s/ Jonathan Shub

Jonathan Shub, Esquire
PA Attorney I.D. #53965
Kevin Laukaitis, Esquire
PA Attorney I.D. #321670

134 Kings Highway East, 2nd Floor
Haddonfield, NJ 08033
(856) 772-7200
jshub@shublawayers.com
klaukaitis@shublawayers.com

SCHMIDT KRAMER, P.C.

SCOTT B. COOPER, Esquire
PA Attorney I.D. #70242
209 State Street
Harrisburg, PA 17101
(717) 232-6300
scooper@schmidtkramer.com

**HAGGERTY, GOLDBERG,
SCHLEIFER &
KUPERSMITH, P.C.**

JAMES C. HAGGERTY, Esquire
PA Attorney I.D. # 30003
1835 Market Street, Suite 2700
Philadelphia, PA 19103
(267) 350-6600
jhaggerty@hgsklawyers.com

**JACK GOODRICH &
ASSOCIATES, PC**

JOHN P. GOODRICH, Esquire
PA Attorney I.D. #49648
To be admitted pro hac vice
Lauren R. Nichols, Esquire
PA Attorney I.D. #313520
To be admitted pro hac vice
429 Fourth Avenue, Suite 900
Pittsburgh, PA 15219
(412) 261-4663

jack@goodrichpc.com
lauren@goodrichpc.com

**PHIL DILUCENTE &
ASSOCIATES, LLC**

PHILIP P. DILUCENTE, ESQUIRE

PA Attorney I.D. #87295

To be admitted pro hac vice

Kenneth Nolan, Esquire

PA Attorney ID #32422

To be admitted pro hac vice

310 Grant Street, Suite 1801

Pittsburgh, PA 15219

412-281-5005

phil@getphil.com

ken@getphil.com

*Attorneys for Plaintiff and the
Proposed Classes*